Amendments to the Claims:

1. A secured communication method for a mobile communications network, the method comprising:

receiving a request to provide a security key to a mobile device connected to the mobile communications network;

generating a unique security key for the requesting mobile device using a public or private key mechanism unless the unique security key is preprogrammed into the mobile device;

storing the unique security key in a first data structure mechanism in association with a unique value identifying the mobile device;

forwarding the unique security key to the mobile device;

storing the unique security key in a second data structure mechanism in the mobile device;

receiving a request to provide the unique security key for the mobile device to a service provider;

approving the request to provide the unique security key based on content of a list of approved service providers, if a first condition is met, wherein the first condition is set by the mobile device; and

providing the unique security key to the service provider, if the service provider is approved to receive the unique security key for the mobile device.

2. The method of claim 1, further comprising:

denying the request to provide the unique security key, if the service provider is not approved to receive the unique security key for the mobile device.

3. (Canceled)

4. (Currently Amended) The method of claim 1~~3~~, wherein the second data storage mechanism is a memory chip.

5. (Currently Amended) The method of claim 1~~3~~, wherein the second data storage mechanism is an identity module for the mobile device.

6. (Currently Amended) The method of claim 1~~3~~, wherein the second data storage mechanism is a SIM card for the mobile device.

7. (Canceled)

8. (Currently Amended) The method of claim 1~~7~~, wherein the unique value is at least one of the mobile device's electronic serial number (ESN), international mobile equipment identity (IMEI) and phone number.

9. (Canceled)

10. (Currently Amended) The method of claim 1~~9~~, wherein the list of approved service providers is stored in the mobile device.

11. (Currently Amended) A security system for managing security key assignment in a mobile communications network~~terminal~~, the security system comprising:

a key generating mechanism for generating a unique security key for a mobile device using a public or private key mechanism unless the unique security key is preprogrammed into the mobile device, in response to a request received by the security system from the mobile device;

a transmission mechanism for transmitting the unique security key to the mobile device; ~~and~~

a first data storage mechanism for storing the unique security key for the mobile device in association with an identifier identifying the mobile device;

a second data storage mechanism for storing the unique security key in the mobile device; and

a verification mechanism for verifying whether a service provider is an approved service provider before the unique security key is transmitted to the service provider based on content of a list of approved service providers, if a first condition is met, wherein the first condition is set by the mobile device and communicated to the security system,

wherein the unique security key is transmitted to thea service provider, in response to a request submitted by the service provider to the security system.

12. (Canceled)

13. (Canceled)

14. (Canceled)

15. (Canceled)